REGIÃO ADMINISTRATIVA ESPECIAL DE MACAU

Lei n.º /2018

(Proposta de lei)

Lei da cibersegurança

A Assembleia Legislativa decreta, nos termos da alínea 1) do artigo n.º 71 da Lei Básica da Região Administrativa Especial de Macau, para valer como lei, o seguinte:

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objecto

A presente lei estabelece o sistema de cibersegurança da Região Administrativa Especial de Macau, doravante designada por RAEM, e regula o seu funcionamento, com o objetivo de salvaguardar os interesses públicos especialmente relevantes, tais como o bem-estar, a segurança ou ordem pública, através de intenficação da segurança cibernética dos operadores de infra-estruturas críticas.

Artigo 2.º
Definições

Para efeitos da presente lei, entende-se por:

1) «Redes informáticas», o dispositivo ou dispositivos que integram um sistema informático, as redes que suportam a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, trocados ou transmitidos por tais dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

2) «Sistema informático» e «dados informáticos», os sistemas e dados previstos na Lei n.º 11/2009 (Lei de Combate à Criminalidade Informática);
3) «Cibersegurança», a actividade permanente e plurisectorial desenvolvida pela RAEM com o objectivo de preservar a operacionalidade, integridade e disponibilidade das redes e dos sistemas informáticos utilizados pelos operadores de infra-estruturas críticas, bem como a confidencialidade dos dados informáticos, e de prevenir através de instrumentos tecnicamente adequados, tais como sistemas de encriptação, "*firewalls*", mecanismos de autenticação e anti-intrusão, em geral, aplicações anti-vírus e instrumentos que impeçam a negação de serviço, que tais redes, sistemas e dados sejam prejudicados ou por qualquer forma afectados por actos não autorizados;
4) «Infra-estruturas críticas», patrimónios, redes e sistemas, que se consideram relevantes para o interesse da sociedade e para o seu funcionamento normal, independentemente da natureza pública ou privada dos respectivos operadores, e cujo dano, revelação dos dados ou perda da função é susceptível de causar prejuízos graves para o bem-estar, a segurança ou ordem públicas ou para outro interesse público especialmente relevante;
5) «Operadores das infra-estruturas críticas», entidades, públicas ou privadas, que operam infra-estruturas críticas e que prestam serviços ligados às mesmas;
6) «Acto não autorizado», qualquer tipo de comportamento que se consubstancie no acesso ou interferência não consentidos nem permitidos pelos proprietários das redes ou dos sistemas informáticos ou por titulares do direito dessas redes ou sistemas;
7) «Incidente de cibersegurança», qualquer situação que configure um acto ou uma tentativa de acto não autorizado;
8) «Operadores de redes», as entidades habilitadas a explorar redes públicas de telecomunicações fixas ou móveis e a prestar serviços de acesso à *internet*.

Artigo 3.º

Actividade de cibersegurança

A actividade de cibersegurança é prosseguida mediante:

1) A definição de orientações, objectivos de ordem geral e de estratégias com vista à prossecução das finalidades da cibersegurança;

2) A implementação, pelos operadores de infra-estruturas críticas, dos deveres e medidas de cibersegurança de rotina definidos na presente lei e nas instruções ou circulares emitidas pelas entidades de supervisão;
3) A implementação de deveres e de medidas de cibersegurança excepcionais, que visem a resposta a incidentes de cibersegurança, em especial nos casos de incidentes graves;
4) A monitorização dos dados relativos à cibersegurança dos operadores de infra-estruturas críticas;
5) A fiscalização do efectivo cumprimento dos deveres e medidas de cibersegurança e a instauração dos correspondentes procedimentos sancionatórios.

Artigo 4.º

Âmbito subjectivo de aplicação

Estão sujeitos aos deveres de cibersegurança:

1) Os operadores públicos de infra-estruturas críticas, compreendendo todos os serviços, órgãos e entidades públicos da RAEM, incluindo:
   (1) O Gabinete do Chefe do Executivo, os gabinetes dos titulares dos principais cargos do Governo e os respectivos serviços de apoio administrativo, os serviços de apoio à Assembleia Legislativa, o Gabinete do Presidente do Tribunal de Última Instância, o Gabinete do Procurador, o Gabinete do Comissariado Contra a Corrupção e o Gabinete do Comissariado da Auditoria;
   (2) Institutos públicos e fundos autónomos, qualquer que seja a modalidade que estes revistam;
   (3) Demais serviços e organismos públicos que, embora desprovidos de personalidade jurídica, possuam autonomia patrimonial e financeira;
2) Os operadores privados de infra-estruturas críticas, compreendendo:
   (1) Todas as entidades de direito privado, com sede na RAEM ou no exterior, habilitadas a exercer actividades nos domínios a seguir especificados, seja a título de concessão de exploração, de prestação de serviços à Administração ou de licenciamento, alvará ou título de idêntica natureza:

(i) Abastecimento de água;
(ii) Actividades bancária, financeira e seguradora;
(iii) Prestação de cuidados de saúde em hospitais;
(iv) Tratamento de águas residuais, recolha e tratamento de resíduos;
(v) Abastecimento público grossista em geral de combustíveis e de produtos alimentares sujeitos a controlos sanitários e fitossanitários;
(vi) Abate de animais em matadouros legais;
(vii) Fornecimento e distribuição de electricidade e gás natural;
(viii) Prestação de serviço público de transportes marítimos, terrestres e aéreos realizados com regularidade, segundo itinerários, frequência de viagens, horários e preços previamente definidos;
(ix) Exploração de portos, terminais marítimos, aeroportos e heliportos;
(x) Difusão televisiva e sonora;
(xi) Exploração de jogos de fortuna e azar em casino;
(xii) Exploração de redes públicas de telecomunicações fixas ou móveis e prestação de serviços de acesso à *internet*;

(2) As sociedades comerciais de capitais exclusivamente públicos;

(3) As pessoas colectivas privadas qualificadas de utilidade pública administrativa nos temos legais.

Artigo 5.º

Exclusões e isenção

1. O disposto na presente lei não se aplica:
   1) Aos serviços, órgãos ou entidades públicos da RAEM que não utilizem redes ou sistemas informáticos, ou que apenas utilizem redes e sistemas cuja cibersegurança constitua responsabilidade de outras entidades públicas, nos termos das disposições dos diplomas orgânicos aplicáveis ou de despacho do Chefe do Executivo;
   2) Aos operadores de difusão televisiva e sonora, cuja actividade se cinja à difusão de conteúdos de entretenimento;

3) Às pessoas colectivas privadas qualificadas de utilidade pública administrativa nos termos legais, cujas finalidades se relacionam com as actividades filantrópicas, assistenciais, educativas, culturais e/ou recreativas.

2. Estão isentos do cumprimento dos deveres previstos na presente lei os operadores privados de infra-estruturas críticas em qualquer das seguintes situações:

1) Não exerçam a actividade para a qual tenham sido licenciados, enquanto essa situação se mantiver, desde que o diferimento do início ou a suspensão da actividade tenha sido antecipadamente comunicado à entidade licenciadora;
2) Sejam isentados desse cumprimento, mediante despacho do Chefe do Executivo, desde que demonstrem plenamente, com os devidos fundamentos, que não usam sistemas e redes informáticas na sua atividade ou que o bom e regular desempenho das suas missões e tarefas não está dependente da permanente operacionalidade dos sistemas e redes informáticas.

CAPÍTULO II
Disposições institucionais

Artigo 6.º
Enquadramento institucional

Integram o sistema de cibersegurança da RAEM as seguintes entidades:

1) Comissão Permanente para a Cibersegurança, doravante designada por Comissão Permanente;
2) Centro de Alerta e Resposta a Incidentes de Cibersegurança, doravante designado por CARIC;
3) Entidades de supervisão de cibersegurança.

Artigo 7.º
Comissão Permanente para a Cibersegurança

A Comissão Permanente é o órgão decisório do Governo, ao qual cabe:

1) Assegurar a actividade referida na alínea 1) do artigo 3.º;

2) Propor ao Governo a celebração e revisão de acordos, protocolos ou contratos com entidades públicas ou privadas, da RAEM ou do exterior, que se mostrem adequados à obtenção de padrões mais elevados de cibersegurança na RAEM.

Artigo 8.º

Centro de Alerta e Resposta a Incidentes de Cibersegurança

1. O CARIC integra as entidades públicas com competências técnicas específicas em matéria de cibersegurança e é coordenado pela Polícia Judiciária.

2. Sem prejuízo do regime de competências e da autoridade da Polícia Judiciária, o CARIC tem as seguintes atribuições:

1) Assegurar a actividade referida na alínea 3) do artigo 3.º, centralizando, para o efeito, a recepção dos alertas sobre incidentes de cibersegurança e coordenando a cooperação e acções adequadas entre as diversas entidades intervenientes, bem como cooperando com as entidades congéneres do exterior, de modo a evitar ou mitigar os efeitos dos incidentes de cibersegurança;
2) Definir e divulgar junto de todos os intervenientes no sistema de cibersegurança os níveis de gravidade dos incidentes de cibersegurança, as instruções e o procedimento das acções de alerta e resposta a incidentes, nos termos das orientações elaboradas pela Comissão Permanente;
3) Monitorizar, através da Polícia Judiciária, em tempo real, o tráfego e as características dos dados informáticos transmitidos sob a forma de linguagem máquina, entre as redes dos operadores de infra-estruturas críticas e a internet, com a finalidade de prevenir, detectar e combater os ataques e invasões cibernéticos;
4) Emitir, quando necessário, alertas sobre incidentes de cibersegurança.

Artigo 9.º

Entidades de supervisão de cibersegurança

1. As entidades de supervisão de cibersegurança são as entidades públicas que prosseguem as atribuições de supervisão em matéria de cibersegurança, perante os operadores de infra-estruturas críticas.

2. As atribuições referidas no número anterior são prosseguidas:

1) Pela Direcção dos Serviços de Administração e Função Pública, doravante designada pelos SAFP, relativamente aos operadores públicos de infra-estruturas críticas;
2) Pelas demais entidades públicas designadas por regulamento administrativo, relativamente aos operadores privados de infra-estruturas críticas.

CAPÍTULO III
Deveres de cibersegurança

Artigo 10.°
Deveres de carácter orgânico

1. Constituem deveres dos operadores privados de infra-estruturas críticas, no âmbito da respectiva organização:

1) Dotar a estrutura operacional das unidades de gestão da cibersegurança e designar os respectivos responsáveis para implementar, com recurso aos meios humanos, financeiros, materiais e patrimoniais, as medidas internas de protecção da cibersegurança;
2) Verificar a idoneidade e a experiência profissional do principal responsável pela cibersegurança dos operadores de infra-estruturas críticas, solicitando obrigatoriamente, para esse efeito, parecer à Polícia Judiciária;
3) Estabelecer mecanismos e meios de reclamações e denúncias relativas à cibersegurança.

2. Para efeitos do disposto na alínea 2) do número anterior, considera-se não possuir idoneidade para o exercício das funções do principal responsável pela cibersegurança, quem for condenado por tribunais da RAEM ou do exterior, por sentença transitada em julgado, por qualquer dos seguintes crimes:

1) Por crimes previstos na Lei n.° 2/2009 (Lei relativa à defesa da segurança do Estado);

2) Por crimes informático ou de falsificação de notação técnica, danificação ou subtracção de notação técnica, devassa por meio de informática, aproveitamento indevido de segredo, violação de segredo de correspondência ou telecomunicações ou violação de segredo profissional;
3) Por qualquer outro crime punível com pena de prisão superior a cinco anos.

3. No caso previsto na alínea 3) do número anterior, as sentenças proferidas por tribunal do exterior da RAEM apenas produzem os efeitos estatuídos nas alíneas 2) e 3) do número anterior, quando os respectivos actos constituam também crimes nos termos da legislação da RAEM.

4. O principal responsável pela cibersegurança deve ter residência habitual na RAEM para estar contactável, a qualquer momento, pelo CARIC, devendo, em caso de ausência ou impedimento, assegurar a sua substituição por outro interlocutor que seja habilitado e conhecedor dos sistemas e contactável pelo CARIC, devendo o mesmo interlocutor aguardar a respectiva colocação na RAEM.

Artigo 11.º

Deveres de carácter procedimental, preventivo e reactivo

1. Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de procedimentos e de prevenção, monitorização e resposta a incidentes de cibersegurança:

1) Estabelecer um regime de gestão da cibersegurança e inerentes procedimentos operacionais internos;
2) Implementar, conforme o regime de gestão da cibersegurança e as circulares e outras instruções emitidas pelas entidades de supervisão, medidas internas de protecção, monitorização, alerta e resposta a incidentes de cibersegurança, nomeadamente:
   (1) Prevenindo que a rede ou os dados que nela circulam sejam prejudicados ou por qualquer outra forma afectados por actos não autorizados, designadamente de acesso, adicionamento, utilização, alteração, controlo, invasão, interferência, revelação, danificação ou destruição;

(2) Informando o CARIC da ocorrência de incidentes de cibersegurança e dando conhecimento do facto à respectiva entidade de supervisão, bem como iniciando, simultaneamente, as acções de resposta a incidentes caso estes sejam classificados como graves;

(3) Monitorizando e efectuando os registos do estado de funcionamento da rede.

2. As circulares e instruções referidas na alínea 2) do número anterior são publicadas no *Boletim Oficial da Região Administrativa Especial de Macau* ou entregues por protocolo ou expedidas sob registo postal com aviso de recepção.

Artigo 12.º

Deveres de auto-avaliação e relato

Constituem deveres dos operadores privados de infra-estruturas críticas, em matéria de auto-avaliação e relato:

1) Proceder, por si próprios ou através de entidades profissionais a quem deleguem, a avaliação da segurança e dos riscos existentes na sua rede;
2) Submeter anualmente à respectiva entidade de supervisão um relatório de cibersegurança, mencionando, designadamente, os eventuais incidentes registados, os resultados da avaliação referida na alínea anterior e as medidas de melhoramento tomadas.

Artigo 13.º

Dever de colaboração

Constituem deveres dos operadores privados de infra-estruturas críticas, bem como da respectiva administração, gerentes ou mandatários:

1) Permitir a entrada dos representantes designados pelo CARIC e pelas entidades de supervisão nas suas instalações, facultar-lhes o acesso às suas redes, na medida necessária à verificação do cumprimento dos deveres referidos no artigo 11.º, e prestar-lhes as informações que estes fundadamente solicitem no âmbito das suas funções;
2) Prestar o apoio e a colaboração necessários para garantir a boa gestão da cibersegurança.

Artigo 14.º

Deveres dos operadores públicos de infra-estruturas críticas

1. Constituem deveres dos operadores públicos de infra-estruturas críticas:
   1) Designar, de entre o pessoal de direcção ou equiparado, um responsável pela cibersegurança, ao qual cabe implementar, com recurso aos meios humanos, financeiros, materiais e patrimoniais, as medidas internas de protecção da cibersegurança;
   2) Cumprir e fazer cumprir os deveres previstos nos artigos 11.º a 13.º, quer internamente, quer no âmbito dos serviços, órgãos ou entidades públicos cuja cibersegurança constitua sua responsabilidade;
   3) Monitorizar a boa execução do contrato de prestação de serviços de cibersegurança celebrado, mediante autorização prévia do Chefe do Executivo, com a entidade privada, sendo o respectivo prestador substituído, quando necessário, pelo operador, no caso de incumprimento do contrato, e sem prejuízo das responsabilidades que ao prestador vierem a ser imputadas.

2. Os operadores públicos de infra-estruturas críticas que não integrem o CARIC apresenta, anualmente, aos SAFP um relatório de avaliação da segurança e dos riscos existentes na sua rede.

CAPÍTULO IV
Regime sancionatório e advertência

Artigo 15.º

Infracções administrativas e respectiva responsabilidade

1. Sem prejuízo de outra responsabilidade que ao caso couber, a violação, por acção ou omissão, dos deveres previstos nos artigos 10.º a 13.º constitui infracção administrativa, sendo aplicada a multa de 150 000 a 5 000 000 patacas, salvo o disposto no número seguinte.

2. Tratando-se de violação dos deveres previstos na alínea 3) do n.º 1 do artigo 10.º, na alínea 2) do artigo 12.º e na alínea 2) do artigo 13.º ou dos deveres estabelecidos pelas entidades de supervisão e comunicados através das instruções ou circulares referidas na alínea 2) do artigo 3.º, é aplicada a multa de 50 000 a 150 000 patacas.

3. Os operadores de infra-estruturas críticas são responsáveis pela prática das infracções administrativas previstas na presente lei, ainda que a respectiva cibersegurança seja, por sua escolha, assegurada por terceiros, e a respectiva responsabilidade não depende da concreta identificação do agente de cuja acção ou omissão resultou a prática da infracção administrativa, nem, sendo o agente individual identificável, da relação entre o agente e o operador de infra-estruturas críticas ou o prestador de serviços de cibersegurança por este escolhido.

Artigo 16.º

Sanções acessórias

1. Pelas infracções ao disposto nas alíneas 1) e 2) do n.º 1 do artigo 10.º, no n.º 1 do artigo 11.º, na alínea 1) do artigo 12.º e na alínea 1) do artigo 13.º, podem ser aplicadas aos operadores privados de infra-estruturas críticas, isolada ou cumulativamente, as seguintes sanções acessórias:

1) Privação do direito de participar em concursos públicos que tenham por objecto a aquisição de bens ou serviços por serviços, órgãos e entidades públicos;
2) Privação do direito a subsídios ou benefícios concedidos por serviços, órgãos e entidades públicos.

2. As sanções acessórias referidas no número anterior, têm a duração máxima de dois anos, contados a partir da data do início da execução das mesmas.

Artigo 17.º

Advertência

1. Caso se verifique a suspeita do incumprimento dos deveres previstos nos artigos 10.º a 13.º pelo operador privado de infra-estrutura crítica, a entidade de supervisão pode adverti-lo para sanar a irregularidade dentro dum prazo fixado, salvo se:

1) A situação consubstanciar um perigo substancial para a cibersegurança;
2) O operador visado tiver sido punido por infracção administrativa de idêntica natureza há menos de um ano.

2. Na falta da sanação da irregularidade pelo operador privado no prazo referido no número anterior, a entidade de supervisão instrui o processo sancionatório relativamente à respectiva infracção.

Artigo 18.º
Reincidência

1. Para efeitos da presente lei, considera-se reincidência a prática de infracção administrativa prevista no artigo 15.º no prazo de um ano após a decisão sancionatória administrativa se ter tornado inimpugnável e desde que entre a prática da infracção administrativa e a da anterior não tenham decorrido mais de cinco anos.

2. Em caso de reincidência, o valor mínimo da multa é elevado de um quarto e o valor máximo permanece inalterado.

Artigo 19.º
Cumulação de sanções

Caso a respectiva conduta constitua simultaneamente infracção administrativa aos deveres de cibersegurança e aos previstos noutra legislação, o infractor é punido de acordo com a legislação que estabeleça multa de limite máximo mais elevado para essa conduta, sem prejuízo da aplicabilidade dos diversos diplomas legais que prevejam a revogação ou suspensão de licenças ou títulos equivalentes e/ou outras sanções acessórias.

Artigo 20.º
Competência sancionatória

1. Compete às entidades referidas no artigo 9.º, relativamente aos operadores privados de infra-estruturas críticas sujeitos à sua supervisão, instaurar os procedimentos sancionatórios previstos nos artigos 15.º a 17.º e instruir os respectivos processos.

2. Compete ao responsável máximo da entidade de supervisão determinar a instauração do procedimento sancionatório, designar instrutor e aplicar sanções.

Artigo 21.º

Cumprimento do dever omitido

Sempre que a infracção resulte da omissão de um dever, a aplicação da sanção e o pagamento da multa não dispensam o infractor do seu cumprimento, se este ainda for possível.

Artigo 22.º

Responsabilidade dos trabalhadores dos operadores públicos de infra-estruturas críticas

1. Sem prejuízo de outra responsabilidade que ao caso couber, os trabalhadores dos serviços, órgãos e entidades públicos da RAEM são disciplinarmente responsáveis pelas infracções aos deveres previstos no artigo 14.º.

2. Quando não seja susceptível de inviabilizar a manutenção da situação jurídico-funcional, as infracções disciplinares por violação dos deveres de carácter procedimental, preventivo e reactivo são puníveis com pena de suspensão de 10 a 240 dias.

CAPÍTULO V
Disposições transitórias e finais

Artigo 23.º

Módulos de identificação de assinante adquiridos antes da entrada em vigor da presente lei

1. No prazo de 60 dias após a entrada em vigor da presente lei, os operadores de redes devem diligenciar no sentido de obter e registar a identidade dos utilizadores de módulos de identificação de assinante, doravante designados por cartões SIM, não sujeitos à prévia identificação e adquiridos na modalidade de pré-pagos, antes da entrada em vigor da presente lei.

1.ª versão enviada à AL

2. Os adquirentes ou utilizadores dos cartões SIM devem fornecer a sua identidade no prazo de 60 dias após solicitada pelos operadores de redes.

3. A partir da data do termo do prazo referido no número anterior, os operadores de rede devem desactivar os cartões SIM, caso os respectivos utilizadores não cumpram o dever de identificação, sem prejuízo da suspensão de serviços que ocorra por virtude do termo da validade dos próprios cartões.

4. O incumprimento pelos operadores de redes dos deveres previstos nos n.^{os} 1 e 3 constitui infracção administrativa, punível nos termos do diploma legal que estabelece o regime de acesso e exercício da actividade de prestação de serviços de *internet*, com a multa de montante mais elevado fixado nesse diploma.

Artigo 24.º

Obrigatoriedade de identificação dos clientes

1. Os operadores de redes devem verificar e registar a identidade dos clientes no momento da celebração de contratos ou da confirmação da prestação de serviços para acesso à *internet*, registo de nomes de domínio ou serviços públicos de telecomunicações fixas ou móveis.

2. É correspondentemente aplicável o disposto no n.º 4 do artigo anterior.

Artigo 25.º

Aditamento à Lei n.º 11/2009

É aditado à Lei n.º 11/2009 o artigo 15.º-A, com a seguinte redacção:

«Artigo 15.º-A

Conservação e fornecimento de registos de tradução de endereços de rede

1. Os prestadores de serviços de *internet* estão obrigados a conservar, por um ano, os registos de tradução de endereços de rede privada em endereços de rede pública.

2. O incumprimento do dever previsto no número anterior constitui infracção administrativa, punível nos termos do diploma legal que estabelece o regime de acesso e exercício da actividade de prestação de serviços de *internet*, com a multa de montante mais elevado fixado nesse diploma.

3. A autoridade judiciária competente pode, quando necessário, ordenar o fornecimento dos registos referidos no n.º 1, observando-se, para o efeito, o disposto nos n.ºs 1 a 4 do artigo anterior.»

Artigo 26.º

Direito subsidiário aplicável

1. Aos actos administrativos previstos na presente lei são subsidiariamente aplicáveis o Código de Procedimento Administrativo e o Código de Processo Administrativo Contencioso.

2. Às infracções administrativas previstas na presente lei são aplicáveis, subsidiária e sucessivamente, as disposições constantes do Decreto-Lei n.º 52/99/M, de 4 de Outubro (Regime geral das infracções administrativas e respectivo procedimento) e, com as necessárias adaptações, as disposições do Código do Procedimento Administrativo e os princípios gerais do direito e do processo penal.

Artigo 27.º

Regulamentação complementar

A regulamentação complementar necessária à execução da presente lei, nomeadamente no que diz respeito às seguintes matérias, é aprovada pelo Chefe do Executivo mediante regulamento administrativo ou despacho regulamentar externo:

1) Definição da composição, competências e modo de funcionamento da Comissão Permanente e do CARIC;
2) Indicação das entidades de supervisão referidas na alínea 2) do n.º 2 do artigo 9.º, tendo em conta a natureza ou o âmbito de actividades responsáveis pelas entidades referidas na alínea 2) do artigo 4.º e as orientações previstas na Lei n.º 2/1999 (Lei de Bases da Orgânica do Governo) e no Regulamento Administrativo n.º 6/1999 (Organização, competências e funcionamento dos serviços e entidades públicos).

Artigo 28.º

Entrada em vigor e produção de efeitos

1. A presente lei entra em vigor 180 dias após a sua publicação.

2. O disposto no artigo 25.º produz efeitos a partir de de de 201....

Aprovada em de de 2018.

O Presidente da Assembleia Legislativa, _____

Ho Iat Seng

Assinada em de de 2018.

Publique-se.

O Chefe do Executivo, _____

Chui Sai On